1. Personal data protection in Poland

In Europe, the issue of the personal data protection is settled by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. It remains in force until May 25, 2018 – at which date its regulations would cease to be effective (according to the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016) and would be replaced by modernized regulation, adjusted to contemporary standards of the personal data processing.

Since the Treaty of Lisbon came into force, the rule of protection of the personal data concerning each natural person is also reflected in a regulation fundamental for the European Union which is Treaty on the Functioning of the European Union - article 16 of it constitutes that “everyone has the right to the protection of personal data concerning them”.

In Poland, the issue of the personal data protection was settled for the first time in 1997 - in article 51 of the Constitution of the Republic of Poland of April 2, 1997 - and comprehensively - in the Act of August 29, 1997 on the personal data protection.

Besides the Act on the personal data protection - in the Polish legal system there are also regulations (implementing regulations to the aforementioned Act) of which the most important for an entrepreneur processing personal data are the regulation of the Minister of the Interior and Administration of April 29, 2004 on the documentation of the personal data processing and technological and organizational conditions which shall be met by devices and IT systems used for the personal data processing, and the regulation of the Minister of the Interior and Administration of December 11, 2008 on the sample of
the declaration form necessary for the registration of personal data filing system to the Inspector General for Personal Data Protection and the regulation of the Minister of Administration and Digitization of December 10, 2014 on the sample of the declaration form necessary for appointment and dismissal of information security administrator.

2. Basic definitions and concepts concerning the personal data protection

**Personal data** - information about natural persons. The information concerns a person identified or identifiable directly (e.g. on the basis of data possessed by the controller) or indirectly (on the basis of data which can be relatively easily acquired by the controller - without spending much time, money or taking many actions).

There is no statutory list of personal data, however it is concluded that the following shall be particularly considered as personal data: an identification number, factors concerning physical, physiological, mental, economic, cultural or social features. The personal data may have an alphabetical or a digital form, may be a photo, a video or a sound or e.g. biometrical data (fingerprint, iris image). E.g. e-mail address may be considered as personal data.

**Sensitive personal data** - a category of personal data demanding special care, the processing of which shall meet more rigorous rules than the processing other categories of personal data. As a matter of principle, the processing of it is forbidden and it is only admitted in the circumstances precisely determined by the legal provisions.

Sensitive personal data is information (exhaustive list) - that disclosure race or ethnical descent, political, religious or philosophical beliefs and faith, party or union affiliation, and information about health condition, genetic code, addictions or sexual life, and information about convictions, judgments ordering punishment and fines, and other judgments pronounced during court or administrative proceedings.

**Data subject** – term defined by the Polish Act on the personal data protection - any natural person, regardless of his or her nationality, age or capacity to perform acts in law. The Act shall not be applied to data concerning a deceased person and (partially) to public data and information made available in the Central Registration and Information on Business.

**Processing of personal data** - shall mean any operation performed upon personal data from its collection until its erasure, such as e.g. collection, recording, storage, adaptation or alteration, disclosure, erasure (removal of personal data or its modification which makes the identification of the data subject impossible). The processing may take place in an IT system or be performed by a traditional method (files, indexes, books).

**Personal data controller** - shall mean a private or public entity that determines the purposes and means of the processing of personal data. It may be, for example an organizational entity, public authority or a person.

In case of a company, the controller of personal data shall be the company itself, not its bodies, people who sit in the company’s bodies or perform governing functions. In case of government agencies, local government units as well as government and municipal entities, those bodies are treated as single controller, as long as the data processing serves the same public interest.

The controller determines the kind of data collected, the purposes of processing them and whether it processes them personally or entrusts the processing of data to third parties (for example, outsources such activities).

**The Polish Act shall be applied to the controllers having its seat or a place of residence in the territory of the Republic of Poland, or in a third country (which is not a part of the European**
Economic Area) as long as they process the data using technical means located in the territory of the Republic of Poland. The Act shall not be applied if the technical means located in the Polish territory are used only for data transfer (transit).

**Information security administrator** - a person who has full capacity to perform legal acts and enjoys full civil rights, has not been punished for an intentional criminal offence and is in possession of appropriate knowledge regarding the protection of personal data, which can be appointed by the personal data controller. Their duty is to ensure that regulations on the personal data protection are respected within an organization. The information security administrator reports directly to the head of an organizational unit or to a natural person being the personal data controller. The personal data controller may appoint deputies of the information security administrator.

**Personal data filing system** - shall mean any structural set of personal data, accessible according to specific criteria (personal - such as name, surname, date of birth, or impersonal - e.g. date of the data introduction to the filing system). The set may be decentralized or dispersed functionally. Regard to the personal data processed in IT systems, the Act shall be applied to the data processed both, in the data filing systems and beyond them, however, while processing by a traditional method - processing in the data filing systems is the condition of the Act application.

**Personal data processor** - shall mean an entity processing the personal data, the entity may be the personal data controller himself, a person authorized for the data processing on the controller’s behalf (e.g. an employee whose duty is to process the personal data) or a third party which is entrusted with the processing of personal data on the basis of a written agreement. Such situation appears e.g. in case of outsourcing services. Neither the authorized person, nor the personal data processor can become the controller basing on a data entrustment agreement.

The title of a processor may or may not be bonded to one entity in the regard of one data filing system - it is possible that the controller processes the data partially and entrusts an entity or entities with processing of other parts of the data filing system.

### 3. Obligations of a personal data controller

Personal data controller is an entity responsible for the personal data processing. This means that the controller is entitled to essential rights (determines the purposes and means of the data processing), but on the other hand the controller is burdened with many responsibilities and is obliged to bear with the consequences of the processing of data in the way incompatible with the Act on the personal data protection.

The controller's basic obligations are:
- to meet one of the legal prerequisites of the personal data processing which are determined by the Act (the prerequisites are described in detail in the part 4 of the summary);
- information obligation regarding the data acquisition;
- requirement to maintain special care while processing data in order to protect the interests of the data subjects;
- requirement to secure the data;
- requirement to notify the data filing system to the register kept by Inspector General for Personal Data Protection, with the exclusion of data processing in a data filing system which is excused from the obligation of registration (issues concerning data filing systems registration are described in detail in the part 7 of the summary);
- requirement to keep the documentation regarding the processing of personal data (documentation which the controller is obliged to keep is described in detail in the part 5 of the summary).
Information obligation regarding the data acquisition

Each personal data controller, regardless of the manner of the personal data acquisition (whether acquired from the data subject or a third entity - e.g. by purchase of a database), is obliged to inform the data subject that he or she (the controller) processes his or her (the subject’s) data.

While acquiring data from the data subject - the controller is obliged to inform the subject about:
- the address of the controller’s seat and the full name (if the controller is a natural person, he or she shall provide the subject with information about his or her name, surname and the place of residence);
- the purpose of personal data collection;
- foreseen receivers or categories of data receivers;
- the right to access his or her data and to correct them;
- the obligation to submit the data or lack of the obligation (if there is such obligation, the controller shall provide the data subject with legal basis).

While acquiring data not from the data subject, the personal data controller is obliged to inform the subject, immediately after recording the acquired data, about:
- the address of the controller’s seat and the full name (if the controller is a natural person, he or she shall provide the subject with information about his or her name, surname and the place of residence);
- the purpose of personal data collection;
- scope of the data collected;
- receivers or categories of data receivers;
- the source of the data;
- the right to access his or her data and to correct them;
- the right to file a justified written demand for cessation of the personal data processing due to a special situation;
- the right to raise an objection against the personal data processing, if the controller is going to process them for marketing purposes, or against entrusting the data to another data controller.

Requirement to maintain special care while processing data in order to protect the interests of the data subjects

The personal data controller is obliged to ensure that the processing performed upon personal data by him or her meets the following principles:
- legality - the processing is based on one of the bases determined by the Act on the personal data protection, it is performed in accordance with the rules determined by the Act and remains compatible with other acts (e.g. the processing of personal data of employees shall be in accordance not only with the Act on the personal data protection, but also with the regulations of the Labor Code);
- purposefulness - the proper realization of this principle shall mean that personal data is collected for specified, explicit and legitimate purposes;
- related with the purpose of collection - it is forbidden to process the data in a manner that is incompatible with the purposes for which it was collected;
- content correctness - the controller is obliged to keep the data up to date and accurate;
- appropriateness - the extent of processed personal data shall be appropriate for the purpose for which it was collected; it is forbidden to process personal data in the extent that exceeds the extent necessary for the realization of the processing purpose.
- restricted time of processing - the personal data may be processed only as long as it is indispensable for the realization of the purpose; when the purpose expires, the data shall be erased.

Requirement to secure the data
The controller is obliged to secure the personal data from disclosure to unauthorized persons, acquiring it by an unauthorized person, processing it in the way incompatible with the applicable regulations, and alteration, loss, damage or erasure. To fulfill this requirement the controller shall apply technological and organizational means appropriate for the category of the processed data and possible threats.

The realization of the requirement bases itself, above all, on the technological protection of personal data, ensuring that the data is processed solely by the persons authorized by the controller, and control of what kind of data, when and by whom was introduced to the data filing system and to whom the data is being disclosed.

Precise regulations on the personal data processing security are determined by the regulations of the Minister of the Internal and Administration of April 29, 2004 on the documentation of personal data processing, and technical and organizational conditions which shall be met by devices and IT systems used for personal data processing (Journal of Laws of 2004, No. 100, item 1024).

4. Bases of personal data processing - legal prerequisites of processing

The entity intending to process personal data is obliged to make sure that at least one of the prerequisites determined by the Act on the personal data protection which legalizes the processing occurs in the case. The Act determines two exhaustive lists - one pointing out situations when it is admissible to process so-called regular personal data, and the second list concerning sensitive personal data.

As a matter of principle, processing of personal data is admissible only when at least one of the following prerequisites occurs:

- the data subject gave the consent to process their data - the consent shall be explicit and expressed intentionally, it may not be alleged or implied from the statement of will with different content (the content is not necessary only for the erasure of the personal data);
- the processing is performed in the accordance with the law which determines entitlements or obligations;
- the processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract,
- it is necessary to perform tasks determined by the legal rule in order to protect public interest;
- it is necessary to fulfill the legally justified purposes performed by the personal data controllers and receivers of the data (legally justified purposes are inter alia direct marketing of one’s goods or the controller’s services, and business activity claims), and the processing shall not violate the rights and freedoms of the subject.

The prerequisites that allow processing of sensitive personal data are more rigorous than the prerequisites which allow processing of other categories of personal data.

As a matter of principle, the processing of sensitive data is forbidden, and admissible only in the following circumstances:

- the data subject gave the consent to process the data (unless this concerns erasure of the data)
  - the consent to process the sensitive personal data shall be given in a written form;
- a legal provision (determined by an Act different than the Act on personal data protection) allows to process data without the subject's consent, and creates additional, full guarantee for protection of such data;
- the processing of the data is necessary to protect vital interests of the data subject or other person (when the data subject is physically or legally incapable of giving the consent - until naming a legal guardian or a trustee);
- it is necessary to fulfill the statutory tasks of churches and denominations, associations, foundations, or other nonprofit organizations or institutions with political, scientific, religious,
philosophical or union objectives - basing the processing on this prerequisite is possible only in
the context of people who participate in such organizations or institutes, or maintain permanent
relations in the connection with their activity; furthermore it is necessary to provide full
guarantees for protection of such data;
- the processing concerns personal data which is necessary for claiming the rights in a court
proceeding;
- the processing in necessary to fulfill the tasks of the controller which are related to the
employment of employees and other people, the extent of the data processing is determined
by the Act;
- the processing is performed with objectives of health status protection, provision of medical
services or curing patients by people who occupy themselves with healing or providing other
medical services, manage medical services distribution, and the full guaranties for personal
data protection are provided;
- the processing concerns personal data which had been disclosed to the public opinion by the
data subject;
- it is necessary to carry out a scientific research, including preparation of a thesis required to
receive a college diploma or an university degree; results of the scientific research may not be
published in the way which makes it possible to identify people whose data have been
processed (anonymization of the results is required);
- the processing of the data is performed by a party with the objective to realize the rights and
obligations resulting from a ruling given in a court or administrative proceeding.

5. Documents of the personal data controller

The personal data processing is attached to the need of keeping the proper documentation by the data
controller. In accordance with the Act on the personal data protection and the regulation of the Minister
of the Interior and Administration of April 29, 2004 on the documentation of personal data, and technical
and organizational conditions which shall be met by devices and IT systems used for personal data
processing, such documentation consists of:
- security policy;
- instruction for managing the IT system;
- documentation on appointing the information security administrator;
- authorizations to process personal data;
- records of people authorized to process the data;
- documents regarding the data filing systems;

Security policy - a document drawn up in a written form by the personal data controller. The obligation
to draw up the document concerns all personal data controllers, regardless of the method applied while
processing data, i.e. either they process data traditionally or using IT systems.

The properly created security policy shall contain inter alia:
- the list of buildings, rooms and their parts which constitute the area where the personal data is
processed;
- the list of personal data filing systems and programs used for the processing of data;
- the description of structure of the personal data filing systems which describes the content of
each information box and the connections between them;
- the method of personal data transfer between particular systems;
- determination of technological and organizational means necessary to ensure confidentiality,
integrity and accountability of the processed data.
The instruction for managing the IT system - the obligation to draw up the instruction for managing the IT system concerns only the controllers that process the data in IT systems. The instruction, like the security policy, shall be drawn up in a written form.

The instruction shall describe in particular:
- procedures of authorizing to process personal data and recording the authorizations in the IT system, and name a person responsible for such activities;
- methods and means applied for authorizing and procedures related with its management and use;
- procedures of initialization, suspension and end of work destined for users of the system;
- procedures of creating backup copies of personal data filing systems, programs and programmed tools used for processing the data;
- the method, place and storage period of electronic data carriers, backup copies of personal data filing systems, programs and programmed tools used for the processing of data, the method of securing the IT system from a software's activity aimed to acquire unauthorized access to the IT system;
- the method of ensuring that the system records information about receivers who get access to the personal data, about the date and extent of the access acquired;
- procedures governing check-outs and maintenance of the system and data carriers used for the data processing.

Documentation on appointing the information security administrator - the information security administrator is a person who can be appointed by the personal data controller responsible for the security of the data processing and authorized to supervise if the requirements concerning the personal data protection established by the controller are fulfilled. The information security administrator is responsible for checking compliance of the personal data processing with the provisions on the protection of personal data and drawing up a report in this regard for the controller and keeping an open register of data files processed by the controller. The personal data controller may entrust fulfilling other duties to the information security administrator. The personal data controller who appointed the information security administrator shall possess the documents attesting it.

The information security administrator shall be a natural person, therefore the personal data controller which is not a natural person may not perform this function. The controller who is a natural person may choose whether to appoint an information security administrator or to perform this function personally.

The law does not determine the relation between the information security administrator and the personal data controller, therefore it is concluded that the administrator may be an employee of the controller or an external entity.

The controller shall ensure the means and organizational autonomy of the information security administrator necessary for him/her to perform his/her tasks. The controller shall be obliged to notify the fact of appointing and dismissing the information security administrator to registration by the Inspector General for Personal Data Protection, within 30 days since the day of his/her appointment or dismissal.

Authorizations to process personal data - the controller of personal data is obliged to secure the data from access of unauthorized persons. Only the persons appointed by the personal data controller i.e. possessing his authorizations, shall be able to access such data.

The regulations do not specify the form of the authorization. For evidence purposes it is recommended that authorization is made in writing. However, it is also possible to grant it via e-mail or even in an oral form (however, it may undermine proving that the authorization was actually granted). In practice, authorizations are mostly used when there are HR or accounting departments within the particular enterprise being the personal data controller.
The authorization to process personal data shall include the following features:
- concern a specific person, indicated by name and surname;
- determine the name and the address of the data controller;
- determine the date of granting the authorization and the date when the authorization shall cease.

It is important to emphasize that the Act does not provide any situation when granting the authorization is not required. Moreover, the authorization to process personal data may not be concluded from the employment agreement nor from the extent of an employee’s obligations.

Records of persons authorized to process the data - the record is a document which shall be kept by all personal data controllers.
The records shall contain at least:
- names and surnames of persons authorized to process the data by the controller;
- dates of granting and dates when the authorization shall cease;
- the extent of each authorization to process personal data;
- ID no. of a user authorized to process personal data (when the data is processed in the IT system).

Documents regarding registration of the data filing systems
At the moment of registration of the filing system containing sensitive personal data in the register kept by Inspector General for Personal Data Protection, the personal data controller shall obtain the attestation of the registration.

The registration of data filing systems which do not contain sensitive data is not confirmed by an attestation issued ex officio by a relevant authority. However, the controller is entitled to file a motion for the attestation.

6. Entrustment of data processing

The personal data controller is entitled to make decisions regarding the personal data which are controlled by him or her, however, there is no legal provision which binds this entitlement with the obligation to process the data personally. What is more, the Act determines precisely the possibility of entrusting the processing of personal data to other entity - agreement on entrustment of personal data processing.

The personal data controller entrusting the processing shall maintain all the entitlements - which means inter alia that only the controller is entitled to decide about purposes and means of the processing. Moreover, the controller can supervise the entity entrusted with the data processing. It shall be emphasized that the entity processing the data on the basis of the entrustment agreement - shall not become the personal data controller - the entity only realizes the will of the data controller and is obliged to follow the controller’s instructions.

The entrustment of personal data processing depends is entirely on the personal data controller. The data subject’s consent is not required to entrust the data. Moreover, there is no obligation to inform the subject about the fact of entrusting the data.

Agreement on entrustment of personal data processing.
The agreement on entrustment of personal data processing shall meet three requirements:
- the agreement shall be concluded in a written form;
- the agreement shall determine the extent of the entrusted data (i.e. determine what kind of data is entrusted - e.g. names, surnames, addresses);
- the agreement shall determine precisely the purpose for which the entrusted data shall be processed (it might be one purpose e.g. data collection or processing with the marketing objectives, but it is possible to entrust all actions related with personal data processing - from its collection to its erasure).

The agreement may additionally determine other issues related to the entrustment of personal data processing, i.e. regulate rules of controls of the data processing carried out by the personal data controller, which certainly would make the cooperation in this regard easier.

Responsibility of the personal data processing entity on the basis of the agreement on entrustment of personal data processing.

The entity is burdened with two kinds of responsibilities - the responsibility resulting from the agreement concluded with the personal data controller and the statutory responsibility.

The contractual responsibility concerns the obligation of the processing entity to follow the personal data controller’s instructions (in particular the instructions regarding the extent and purpose of the data processing). The personal data processing entity, which does not follow the data controller’s instructions, shall bear liability for processing the data in the way incompatible with the agreement.

The entity that processes the data on the basis of the entrustment agreement is also burdened with the obligations determined by the Act - in particular the obligation to secure the data even before the initiation of the processing. This shall mean the necessity to apply technological and organizational means which would secure the data from disclosing them to unauthorized persons, from acquisition, alteration, loss, damage or erasure of the data, and from processing it in the way incompatible with the Act. In this regard, the entity that processes the data on the basis of the entrustment agreement shall share the responsibility with the personal data controller, and the entity's activity may be subject to the audit procedures carried out by Inspector General for Personal Data Protection. The entity may also be the addressee of the decisions issued by the Inspector General for Personal Data Protection.

Responsibility of the personal data controller

The personal data controller shall be fully responsible for the data entrusted for processing - the controller bears liability as if he or she was processing it. This is why the controller’s entitlement to supervise the entity, to which the data are entrusted, and giving the entity instructions is so important.

The personal data controller, while entrusting the data processing is additionally required to disclose this fact in the register kept by Inspector General for Personal Data Protection. The controller may do it while registering the set or later in a data update form.

7. Registration of the data filing systems

The personal data controller is obliged to notify the data filing systems, in which the data is processed, to registration by the Inspector General for Personal Data Protection. Such notification shall be submitted before the initialization of the personal data processing in the data filing system.

The controller who has appointed the information security administrator and notified the latter to registration by the Inspector General for Personal Data Protection, shall not be subject to the obligation of personal data files registration, except for the data filing systems containing sensitive personal data. In such case the register of data filing systems is kept by the information security administrator.

As a matter of principle, personal data processing is legal from the moment of notification of the data filing system to the registration, however, in case of sensitive data - the processing is legal only from the
moment of the data filing system registration confirmed by the attestation of the registration issued by the Inspector General for Personal Data Protection.

The data filing system notification shall be submitted using a declaration form, sample of which is determined by the regulation of the Minister of the Internal and Administration of December 11, 2008 on the sample of the declaration form necessary for the registration of the personal data filing system to the Inspector General for Personal Data Protection (Journal of Laws of 2007, No. 229, item 1536). The declaration may be filled in the Office of the Inspector General for Personal Data Protection located in Warsaw, by email, by post or via the Internet through the e-Giodo website (http://egiodo.giodo.gov.pl).

The update of the data filing system shall be made in the same way as it was notified for registration. The update shall be done within 30 days from the day of alteration (with exception of the data filing systems which contain sensitive data, in the case the alteration may be done only after previous registration of it).

The Act on the personal data protection determines numerous exemptions from the obligation to register, the personal data controllers are not obliged to notify the data filing systems such as:
- data filing systems in which data is processed in the context of the employment and provision of services on the basis of a civil-law agreement;
- processed only for the purpose of issuing invoices, accounts or keeping financial reporting;
- generally accessible;
- processed in the scope of minor daily matters.

8. Inspector General for Personal Data Protection

Inspector General for Personal Data Protection is the body particularly responsible for controlling the processing of personal data, issuing administrative decisions, considering the claims and keeping the register of personal data filing systems and the register of information security administrators.

The Inspector General also carries out execution proceedings, which can result inter alia in levying a single fine on a natural person up to the amount of PLN 10,000 (to the maximum PLN 50,000 total), and a single fine on a legal person up to the amount of PLN 50,000 (to the maximum PLN 200,000 total).

Audits shall be performed by the inspectors of the Office of the Inspector General for Personal Data Protection. The inspectors pay attention, in particular, to:
- the processing compatibility with the law, in particular if the legal prerequisites determined by the Act are met;
- securing the processed data;
- the extent and the purpose of the personal data processing;
- fulfillment of the information obligation by the controlled entity towards the data subjects;
- registration of the personal data filing systems.

When the audit procedures are completed, the inspectors shall create an audit protocol. The controlled entity shall obtain one copy of the protocol and is entitled to raise justified comments and reservations regarding the protocol’s content, and also is entitled to refuse signing the protocol. If, as the result of audit, the inspector detects an infringement of legal provisions governing personal data protection, the inspector shall apply to the Inspector General for issue of a decision obligating the entity to remove the infringement.

9. Transfer of the data abroad

The rules of transferring the data beyond the Polish borders differ depending whether the receiving country is a part of European Economic Area or not.
Transfer of personal data to the countries of European Economic Area

The European Economic Area currently consists of 31 countries - including members of the European Union and Iceland, Norway and Lichtenstein.

In the European Economic Area, the rule of free flow of personal data is applicable. Therefore, the transfer of the data is being performed in accordance with the same rules as governing the national personal data transfer - therefore the requirements determined by the Polish Act on protection of personal data shall be applied.

Transfer of personal data to a third country - which is not a member of the European Economic Area

The transfer of personal data to a third country may be done only if the country of destination ensures an adequate level of personal data protection in its territory. The adequacy of the level of the personal data protection shall be evaluated taking into account all the circumstances concerning a data transfer operation, in particular the nature of the data, the purpose and duration of the proposed data processing operations, the country of origin and the country of final destination of the data as well as the legal provisions being in force in a given third country and the security measures and professional rules applied in this country.

A third country may not give such protection guarantees if the prerequisites determined by the Act are met, e.g. the data subject gave the consent for it in a written form or the consent of Inspector General for Personal Data Protection was acquired (the consent of the Inspector General is not required, if the controller ensures adequate safeguards with respect to the protection privacy, rights and freedoms of the data subject, by means of standard contractual clauses on personal data protection, approved by the European Commission or legally binding personal data protection principles or policies, which were approved by the Inspector General).

10. Responsibility for the data processing in a manner incompatible with the act on personal data protection

The processing of personal data in the way incompatible with the Act on personal data protection results with criminal liability, for:
- processing of the data by an unauthorized person;
- disclosing the data to unauthorized people or granting access to the data;
- violation of the obligation to secure the personal data;
- lack of notification of the data filing system to registration by the Inspector General for Personal Data Protection;
- non-performance of the information obligation towards the data subject;
- making the audit procedures difficult for inspectors of the Office of the Inspector General for Protection of Personal Data.

In each case, the entity responsible for infringements is the personal data controller, in some cases (e.g. not securing personal data) the responsibility may be shared with the processing entity.

The material was prepared and summarized for Polish Information and Foreign Investment Agency by:

Olesinski & Wspolnicy sp.k.
Prosta 32 street
00-838 Warsaw
Currently Olesiński&Wspólnicy means over 80 advisors in 4 Polish cities. 11 years of experience and constantly developing network of relations both with domestic and foreign Partners.

We provide services to the clients from various economic sectors, offering comprehensive legal and tax consulting in all legal areas. Diligently defining expected results, we are looking for solutions and implementing new courageous ideas. While doing so, we take responsibility for the recommended solution, which is the basis of our approach.

Contact:

Grzegorz Leśniewski, manager, attorney

Manager in Olesiński&Wspólnicy, he manages the Warsaw office and leads the TMT team. He is responsible for strategic consulting for initiatives based on blockchain and cloud computing technologies, in particular with reference to the principles of cross-border personal data flow. Coach and speaker and also author of many publications within the scope of his specialization, in particular co-author of the book „Protection of personal data in HR departments. The answers to 370 most difficult questions” released in 2014.

Phone: (+48) 22 12 35 237
E-mail: grzegorz.lesniewski@olesinski.com

Anna Chrobot, partner, attorney

Works in Olesiński&Wspólnicy since 2005. She specializes in the areas connected with maintenance of the business entities in particular in the field of maintenance of the of public procurements. Regardless of that she also specializes in labor law, in particular connected with HR departments, collective labor disputes and employment restructuring. She has long-term professional practice including provision of regular legal service to legal entities with foreign capital in the fields of commercial and tax law.

Phone: (+48) 71 75 00 702
E-mail: anna.chrobot@olesinski.com